(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. Mai 2005 (19.05.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/045685 A1

(51) Internationale Patentklassifikation[7]: G06F 12/14

(21) Internationales Aktenzeichen: PCT/EP2004/012435

(22) Internationales Anmeldedatum:
3. November 2004 (03.11.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 52 401.0 10. November 2003 (10.11.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **MICRONAS GmbH** [DE/DE]; Hans-Bunte-Strasse 19, 79108 Freiburg (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **PLOOG, Hagen** [DE/DE]; Baumkirchener Strasse 25, 81673 München (DE). **STEFFENS, Reinhard** [DE/DE]; Brunnstrasse 11, 80331 München (DE).

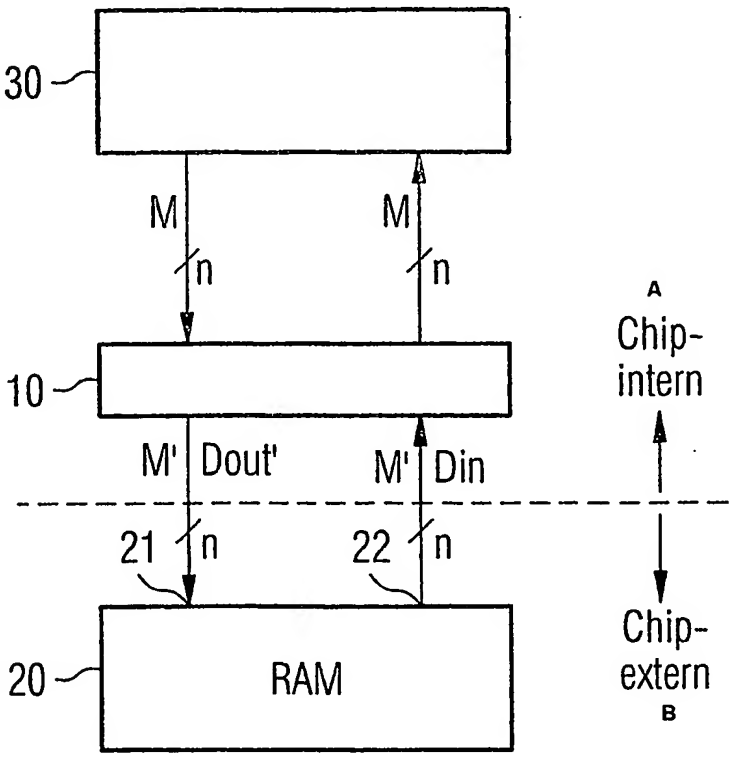
(74) Anwalt: **BICKEL, Michael**; Westphal, Mussgnug & Partner, Mozartstrasse 8, 80336 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

*[Fortsetzung auf der nächsten Seite]*

(54) Title: METHOD FOR STORING DATA IN A RANDOM ACCESS MEMORY AND ENCRYPTION AND DECRYPTION DEVICE

(54) Bezeichnung: VERFAHREN ZUR SPEICHERUNG VON DATEN IN EINEM WAHLZUGRIFFSPEICHER UND VERSCHLÜSSELUNGS- UND ENTSCHLÜSSELUNGSVORRICHTUNG




A...CHIP-INTERNAL
B...CHIP-EXTERNAL

(57) Abstract: The invention relates to a method for storing data in a random access memory and an encryption and decryption device. The method for storing data in a random access memory in which data items comprising a respective determined number of data bits can be stored is characterized in that before storage every data item is encrypted by generating, on the basis of every data item or a data item derived from said data item, a permutated data item having the predetermined number of data bits by one-to-one permutation of the individual data bit using a first permutation key.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Speicherung von Daten in einem Wahlzugriffsspeicher und eine Verschlüsselungs- und Entschlüsselungsvorrichtung. Das Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher, in dem Datenworte, die jeweils eine vorgegebene Anzahl Datenbits umfassen, abspeicherbar sind, sieht vor, dass vor der Speicherung eine Verschlüsselung eines jeden Datenwortes erfolgt, indem aus jedem Datenwort oder einem aus dem Datenwort abgeleiteten Datenwort durch eineindeutiges Permutieren der einzelnen Daten bits unter Verwendung eines ersten Permutationsschlüssels, ein permutiertes Datenwort mit der vorgegebenen Anzahl Datenbits erzeugt wird.

WO 2005/045685 A1

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**
— *mit internationalem Recherchenbericht*

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*